

Cyber Crime: Prevention & Detection

*** Manjugouda R Patil ** Dr. C.F.Mulimani**

*Research scholar, Department of Criminology and Forensic science, Karnatak Science College, Dharwad, Karnataka.

**Research supervisor, Associate professor, Department of Criminology and Forensic science, Karnatak Science College, Dharwad, Karnataka.

ABSTRACT:

Cybercrime is a borderless problem, committed online by using electronic communication networks and information systems. Cyber attacks have evolved in terms of sophistication and reach in the recent times. Attacks are often anonymous and difficult to impute to specific actors, states or non-states. Cyber security is a broad spectrum phrase and related to preventing any form of unauthorized and disingenuous access to a personal computer, a laptop, a Smartphone or major network like the national banking system or a national information technology asset that also has military implications whether it is for e-mail, net banking, WhatsApp or Paytm, almost everyone is dependent on the internet and hence potentially vulnerable. Security becomes a challenge as now privacy is a fundamental right as per Supreme court 's verdict and rise in cyber crimes have lead to the violation of private space and liberty of expression. In this paper, we have discussed the need for new tools, capacity building and mechanism in place to address the challenges. Institutions such as the Computer Emergency Response Team (CERT-In), National Technical Research Organization (NTRO) and National Cyber Security Coordinator Centre are all doing a reasonable job. In this paper, we have also discussed the prevention technique, detention technique and some online safety tips along with National Cyber Security Policy 2013 and Information Technology Act 2000.

KEYWORDS: Cybercrime, Cyber security, Information Technology Act 2000, National Cyber Security Policy 2013, Prevention methods.

1. INTRODUCTION

In our modern technology-driven age, keeping our personal information private is becoming more difficult. The truth is, highly classified details are becoming more available to public databases because we are more interconnected than ever. Our data is available for almost anyone to sift through due to this interconnectivity. This creates a negative stigma that the use of technology is dangerous because practically anyone can access one's private information for a price. Technology continues to promise to ease our daily lives; however, there are dangers of using technology. One of the main dangers of using technology is the threat of cyber crimes.

Common internet users may be unaware of cybercrimes, let alone what to do if they fall victim of cyber attacks. Many innocent individuals fall victim to cybercrimes around the world, especially since technology is evolving at a rapid pace. Cybercrimes are any crimes that cause harm to another individual using a computer and a network. Cybercrimes can occur by issues surrounding penetration of privacy and confidentiality. When privacy and confidential information is lost or interrupted by unlawfully individuals, it gives way to high profile crimes such as hacking, cyber terrorism, espionage, financial theft, copyright infringement, spamming, cyber warfare and many more crimes which occur across borders.

Cyber-attacks have grown in terms of sophistication and reach in the recent times. Attacks are often anonymous and difficult to attribute to specific actors, state or non-state. Advanced Precision Threats (APTs) carried out by anonymous hackers are often silent and go unnoticed for long periods.

2. INDIA'S READINESS AND PERFORMANCE WITH RESPECT TO CYBER THREATS

- The government is stepping up authority around cybersecurity to check the rising menace of financial frauds. Global Conference on Cyberspace was conducted in India for the first time with a view to establishing internationally agreed 'rules of the road' for behavior in cyberspace and create a more focused and inclusive dialogue between all stakeholders on how to implement them.
- The government has earlier launched the Digital Investigation Training and Analysis Centre (DITAC) to tackle these crimes.
- DITACs will monitor and police cyber-crimes committed through different platforms such as mobile, email, computer and social media platforms like Twitter and Facebook.

- Apart from DITACs, the government also established the National Cyber Coordination Centre, an operational cybersecurity and e-surveillance agency in India.

3. CRITICISM OF INDIA'S READINESS

- India emerged as the third most vulnerable country in terms of risk of cyber threats, such as malware, spam, and ransomware, in 2017, moving up one place over the previous year, according to a report by Symantec.
- As per the report, India continues to be the second most impacted by spam and bots, third most impacted by network attacks, and fourth most impacted by ransomware.
- India faces the highest number of cybersecurity threats in the Asia-Pacific region with over 500,000 alerts daily, according to cybersecurity report, Cisco 2018 Asia-Pacific Security Capabilities Benchmark.
- The Indian Computer Emergency Response Team (CERT-In), the governmental nodal agency for dealing with and handling of cybersecurity threats, had less than 1% of the reported number of incidents come from security researchers.
- With the growing adoption of the Internet and smart-phones, India has emerged as one of the favorite countries among cybercriminals.
- India is not a signatory to the Budapest convention which is the only multilateral convention on cybersecurity.

4. DEFINING THE PROBLEM

Cyber Crime is not defined in the Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India. In fact, it cannot be too. Offense or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislation too. Hence, to define cybercrime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offense or crime in which a computer is used is a cybercrime'. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cybercrime, about which we will now be discussing in detail.

5. CAUSES OF CYBERCRIMES

There are many ways or means where cybercrimes can occur. Here are a few causes and methods of how cybercrimes can be committed on a daily basis: Hacking, Theft of information

contained in electronic form, Email bombing, Data diddling, Salami attacks, Denial of Service attack, Virus / worm attacks, Logic bombs, Trojan attacks, Internet time theft, Web jacking etc.

6. MAJOR TYPES OF CYBER ATTACKS

Backdoor

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from the poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability.

Denial-of-service attack

Denial of service attacks (DoS) is designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet, but a range of other techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

Direct-access attacks

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless mice. Even when the system is protected by standard security measures, these may be able to be bypassed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network.

Spoofing

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

Tampering

Tampering describes a malicious modification of products. So-called “Evil Maid” attacks and security services planting of surveillance capability into routers are examples.

Privilege escalation

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. So for example a standard computer user may be able to fool the system into giving them access to restricted data; or even to “become root” and have full unrestricted access to a system.

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Clickjacking

Clickjacking, also known as “UI redress attack” or “User Interface redress attack”, is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically “hijacking” the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully crafting a combination of style sheets, iframes, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

Credit/Debit Card Fraud

It is the unlawful use of a credit/debit card to falsely attain money or belongings. Credit/debit card numbers can be stolen from leaky websites or can be obtained in an identity theft scheme.

Identity theft

This is when someone seizes another's individual information without his or her awareness to commit theft or fraudulent. Typically, the victim is led to believe they are revealing sensitive private data to a genuine business, occasionally as a response to an e-mail to modernize billing or membership information etc.

Ponzi/Pyramid method—this is where investors are lured to capitalize in this falsified arrangement by the promises of irregularly or abnormally high profits but none of the funds are actually made by the so-called “investment firm”.

7. PREVENTION AND PROCEDURE

In this modern age, it seems almost impossible to avoid being a victim of cybercrime, with all the advancements in technology which make it easy for someone to perform cybercrimes. In light of this, there are some ways however to avoid becoming a victim of cybercrime. Most internet browsers email service, and Internet providers provide a spam-blocking feature to prevent unwanted messages, such as fraudulent emails and phishing emails, from getting to your inbox.

However, every user must ensure to turn them on and do not turn them off whatsoever. Also, users must install and keep up-to-date antivirus programs, firewalls, and spyware checkers. Along with keeping them up to date, users must make sure that they run the scans regularly. There are many companies out there that provide free software, but there are others you can purchase, along with that of the many produced by the leading companies providers; in addition, those companies provide a free version of their paid or subscription antivirus software. Encryption of information that you do not want anyone to have unauthorized access to is a good way to avoid some cybercrimes; information such as password and credit card information for example. Encryption software runs your data through encryption algorithms to make it unintelligible to anyone who tries to hack into your computer.

Another good precaution is to be wary of who you divulge your personal information to. Try to avoid unknown websites, in particular, those that ask for your name, mailing address, bank account number or social security number. When doing online shopping make sure website is secure, look for URLs that start with “https” and/or have the Trustee or VeriSign seal. If you do not see these

anywhere on the site, you run the risk of submitting credit card information and other personal information to a site that may be a fraud.

Another way to avoid being a victim of cybercrimes is to avoid being susceptible to common frauds, such as an inferences letter, letter asking for your help in placing large sums of money in overseas bank accounts, foreign lotteries, and phony sweepstakes. Those mentioned activities are all methods used by cybercriminals to get your personal information and money. If it sounds too good to be true, it probably is. Educate children about the proper use of the computer and internet and make sure to monitor their online activities at home and school alike. They should only have access to a computer located in a central area of your home and you should regularly check all browser and email activity.

A wise thing to do is to use parental control software that limits the type of sites the user can gain access to. In schools, there should be restricted websites and other use restrictions that will help protect the user and entity from cybercrime. Likewise, companies should educate and have written policies governing the workplace pc and its network use to diminish the risk of cybercrime against the company. One definite way to ensure that you don't fall, a victim of cybercrimes, is to disconnect your computer entirely from the internet. If there is no network, then you don't have to worry about any cyber-attacks. However, this option is not the most viable one in our interconnected society. The truth is, it is up to you to take the necessary precautions to avoid potential cybercrimes.

Need for comprehensive cybersecurity

1. Economic and governance dependence on the cyber world

- India is one of the key players in the digital and knowledge-based economy, holding more than a 50% share of the world's outsourcing market.
- India is already the third largest hub for technology-driven startups in the world and its Information and Communications Technology sector is estimated to reach the \$225 billion landmark by 2020.
- Pioneering and technology-inspired programmes such as Aadhaar, MyGov, Government e-Market, DigiLocker, Bharat Net, Startup India, Skill India, and Smart Cities are propelling India towards technological competence and transformation.

2. Cyber attacks

- India the fifth most vulnerable country in the world in terms of cybersecurity breaches, according to the Internal Security Threat Report of 2017 by Symantec India.

3. Attacks from private organized and unorganized hackers

- The recent WannaCry ransomware attack (May 2017), which infected more than 2,30,000 computers in over 150 countries, brought the compelling need for cybersecurity policies and laws into sharp focus. This malware infected at least 48,000 computer systems across various organizations in India.
- In India, in May 2017, a data breach at the food delivery App, Zomato, led to personal information of about 17 million users being stolen and put for sale on the Darknet.
- Similarly, hackers stole data from 57 million Uber riders and drivers.
- While Windows operating systems were the most vulnerable to cyber attacks, a number of Android threats have been reported in the last couple of years, including potent crypto-ransomware attacks on Android devices.

4. State-sponsored cyber attacks

- In a series of recent events, a number of countries have witnessed serious incidents wherein outside agencies have attempted to hack networks during general elections and turn cyberspace to a certain strategic advantage or tip election results in favor of a particular party or candidate.
- It is widely believed that the 2016 US presidential election was an easy -target for Russian cyberespionage

Government efforts

- Cybersecurity needs to be integrated into every aspect of policy and planning.
- The second Global Cybersecurity Index, released by the International Telecommunication Union in July, which measured the commitment of nations to cybersecurity, found that India ranked 23 out of 165 nations.

1. National Cybersecurity Policy, 2013

- The NCSP offers a 14-point strategy to establish a secure cyber-ecosystem and assurance framework.
- It centers on the product, process/technology, and the personnel that form the basic building blocks of any cybersecurity system.
- It seeks to promote global best practices in information security (IS) and compliance through standards and guidelines—the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 2001 is the best-known standard in the family

providing requirements for an information security management system (ISMS)—it includes IS system audits, penetration testing and vulnerability assessments, formal risk assessments and risk management processes, as well as a cyber-crisis management plan for all entities within the government and critical sectors.

- The document envisioned the creation of a 5,00,000-person workforce (cyber-warriors) skilled in cybersecurity within five years. However, there appears to be a glaring skill gap in the cybersecurity industry, and to compound the problem, cybersecurity professionals are in great demand in the public as well as private sectors.
- Moreover, there are very few academic programmes on cybersecurity at the university level, and existing curricula do not address emerging trends and challenges.
- The NCSP needs an overhaul to grapple with new technological innovations and, in turn, challenges in the field.

2. Information Technology Act, 2000

- The IT Act, 2000 was designed in response to the increased risk of cyber attacks.
- It seeks to reduce the digital divide to bring about societal transformation.
- The IT Act is umbrella legislation that primarily aims to regulate electronic commerce as well as to gradually promote a culture of e-governance in India.
- It seeks to effectuate the 1997 United Nations Commission on International Trade Law (UNCITRAL) Model Law on E-Commerce and refers to it in its preamble.
- An amendment in 2008 to the act widened the definition of cybersecurity to include “protecting information, equipment, devices, computer, computer resources, communication device, and information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction”
- The law seems to make a reasonable effort to tackle two areas of policy in need of reform: cybersecurity and data privacy.
- However, it lacks detailed architecture to establish an effective cybersecurity system.
- As such, it calls for comprehensive cybersecurity legislation to address growing threats to information infrastructure systems and networks and suggests a new specialized professional institutional structure to meet the cybersecurity challenge.

3. National Technical Research Organisation (NTRO)

- The National Technical Research Organisation (NTRO) is a technical intelligence agency under the National Security Advisor in the Prime Minister's Office, India. It was set up in 2004.
- It also includes National Institute of Cryptology Research and Development (NICRD), which is first of its kind in Asia.
- The agency develops technology capabilities in aviation and remote sensing, data gathering and processing, cyber security, cryptology systems, strategic hardware and software development and strategic monitoring.

4. International Cooperation

- India should foster closer collaboration between all those involved to ensure safe cyberspace.
- There must be enhanced cooperation among nations and reaffirmed a global call to action for all United Nations member nations to not attack the core of the Internet even when in a state of war.
- There is a need for a Geneva-like Convention to agree on some high-level recommendations among nations to keep the Internet safe, open, universal and interoperable.

5. National Critical Information Infrastructure Protection Centre

- GoI established the National Critical Information Infrastructure Protection Centre (NCIIPC) to safeguard critical infrastructure and key resources in 2014.
- The NCIIPC acts as a nodal agency for all measures to protect critical information infrastructure(CII), defined in the IT Act (2000) as “the computer resource, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health, or safety.”

6. CERT-In

- Meanwhile, to handle emergency situations and ensure crisis management, another institution—the Computer Emergency Response Team-India (CERT-In)—has been created.
- It operates 24/7 to help users respond to cybersecurity incidents.
- CERT-In has established links with international CERTs and security agencies to facilitate the exchange of information on the latest cybersecurity threats and international best practices.

7. Defense cybersecurity

- An increase in the volume and scale of cyber attacks on defense infrastructure has heightened the need for cybersecurity.
- A proposal is already pending before the Ministry of Defence to set up a dedicated tri-service command with the Indian Air Force, army and navy for cybersecurity.
- It is time to enhance cyber capabilities so that the defense forces can deploy both defensive and offensive cyber operations to protect vital national interests.

8. Conclusion

Cybercrime will always be an ongoing challenge despite the advancements being made by numerous countries. Most countries have their own laws to combat cybercrimes, but some doesn't have any new laws but solely relies on standard terrestrial law to prosecute these crimes. Along with outdated laws to combat cybercrime, there are still feeble penalties set in place to punish criminals, thus doing no major prevention of cybercrimes' which affect the economy and people's social lives on a large scale by those criminals. Consequently, there is a desperate need for countries on a global scale to come together and decide on what constitutes a cybercrime, and develop ways in which to persecute criminals across different countries.

Remember, cybercriminals are evolving as well in terms of computer knowledge per technological advancement made. Nevertheless, business should employ practices where their employees follow proper safety practices to ensure that integrity and confidentiality of stored information is kept at all times to combat cybercrimes. Safety practices like ensuring that staying off game sites on company time where viruses can be downloaded, forwarding chain emails, leaving workstation unattended or password sharing over virtual mediums should be prohibited. With all these safety practices implemented, it can be said that the safety of many clients stored information is optimal.

References

<https://www.thehindu.com/opinion/op-ed/for-a-safe-cyberspace/article21864764.ece>

<https://www.thehindubusinessline.com/news/to-combat-online-crimes-govt-to-launch-more-cyber-security-labs/article24156735.ece>

<https://www.financialexpress.com/infrastructure/railways/irctcs-cybersecurity-breach-it-is-time-govt-bodies-recognise-and-incentivise-ethical-hacking/1379817/>

http://www.cameron.edu/cybersecurity/research/it4444_2011/2_Hackers.docx

http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

http://www.horizonsfcu.com/content.php?c_id=26

<https://economictimes.indiatimes.com/blogs/et-commentary/cybersecurity-what-india-needs-to-do/>

https://advocatespedia.com/A_critical_analysis_on_need_for_regulation_in_cyberspace

<https://www.thehansindia.com/posts/index/Young-Hans/2017-06-14/Cyber-security-and-challenges/306445>

<https://www.scribd.com/document/370874840/out2>

<http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf>

https://en.wikipedia.org/wiki/Computer_security